REMARKS

Applicants respectfully request reconsideration of the present application in light of the above amendments and the following remarks.

Claims 81 – 89 are pending. The outstanding office action took the position that claims 81 – 85 and 87 – 89 are obvious in view of the '831 patent to Coleman et al. and the '606 patent to Ammon et al, while claim 86 was also deemed obvious in light of these two references in further view of the '741 patent to Bardsley et al. Applicants respectfully request careful consideration of the subject matter of the pending claims and the actual teachings of the cited references.

Initially, Applicants' present invention is directed to detecting/identifying an interloper/spoofing attack on a wireless network. Such an attack may involve one or more attackers. For example, a "wolf pack" comprising a plurality of rogue client attackers may stage a coordinated, simultaneous or substantially simultaneous, attack on a wireless network. In the following discussions, authorized clients are referred to as non-rogue clients while unauthorized interlopers are referred to as rogue clients. The abbreviation AP is used in this amendment to refer to an access point which is a base station e.g. a Wi-Fi (802.11) base station. The non-rogue clients refer to authorized communication devices being serviced by the base station.

In Applicants' claimed inventions a single antenna array (in an apparatus comprising one or more such antenna arrays) receives a communication beam packet comprising a single source address. In Applicants' invention, a source address is important because multiple members of a wolf pack may try to gain access using the

same source address, or attempt to intercept communications from non-rogue clients and then may use the non-rogue clients source addresses. By associating a single source address with propagation-specific properties of received communication beam packets, such as multipath channel responses, time-delays-of-arrival, received signal strengths, and or angles-of-arrival, Applicants' invention provides an interloper identification process with high-sensitivity. By way of non-limiting example, if a specific antenna array in Applicants' claimed apparatus receives two communication beam packets bearing the same source address within a certain temporal window and if the monitored propagation-specific properties would not permit the level of discrepancy between those monitored propagation-specific properties within that temporal window, then those communication beam packets are deemed to emanate from an interloper and actions can be taken to deny access/service. The type of action take can be determined by the system designer/operator. Thus, it can be seen that the monitoring of received signal characteristics relating to a single source address at a given antenna array is central to Applicants' claimed invention. None of the cited references teach or suggest monitoring at least one received signal characteristic of communication beam packets received at a single antenna array for plurality of received packets that relate to a single source address.

The Coleman patent uses location/direction-of-arrival in both its rogue identification and rogue countermeasure procedures (see Coleman Fig. 8), with the first part of the patent detailing how its smart-antennas deny service to a rogue (based on an incoming direction-of-arrival). The second part of the patent in the description of an

"Adaptive Learning Detection System" (cf. text following col. 16, line 27) suggests how it might identify a rogue, using direction of arrival inputs. See the flowchart in Figure 8 of Coleman, which apparently presumes prior existing knowledge of the location of a (non-rogue) client. No specific mention of source addresses is made anywhere in Coleman. As the Office Action notes in the citation of col. 11, lines 35 – 44, Coleman uses behaviors (from 'wireless events') that are profiled against

a) cataloged attack behaviors

b) known good behaviors (to assess anomalies).

to establish 'mistrust levels' and alarms that can eventually blacklist emitter directions (for countermeasures).

Coleman, in effect, treats the rogue-client as a jammer/eavesdropper---and tries to deny servicing the rogue client by having each AP (within a service range) place an antenna pattern null in the direction of the rogue client. (Each AP has a smart antenna that can spatially adapt both its transmission and reception patterns.) Eavesdropping by the rogue is thwarted, because, due to nulling, it cannot (subsequently) easily receive transmissions from any AP; jamming by the rogue is thwarted because it cannot interfere with communications to the AP from non-rogue clients (since an AP's receiver response in the rogue's direction is attenuated by 'smart processing').

The secondary reference relied upon in the proposed combination, namely Ammon et al., is a network/protocol-focused patent. Ammon does not focus on the characteristics of communication beam packets received at a single, given access point (antenna array). While Ammon mentions source addresses, his disclosed system sniffs

for protocol anomalies by **network-coordinated** means to detect 'copycat' spoofing which may involve attacks on different APs. Ammon does not teach or suggest utilizing the available physical layer/spatial aspects of a communication beam packet received at a **single AP** like Applicants' claimed invention which greatly increases discrimination **by that AP alone**. Ammon does not "teach or suggest" correlating physical aspects of beam packets having a single source address with received signal characteristics for signals received at a single AP for interloper detection.

Since neither of the Coleman nor Ammon references teach or suggest the subject matter claimed in amended independent claim 81, dependent claims 82 – 89 are also patentable over the cited references.

CONCLUSION

Applicants respectfully submit that all pending claims are in condition for allowance. If the Examiner has any questions or comments which may expedite the prosecution of this application, he is respectfully requested to contact Applicants' attorney at the telephone number set forth below.

Respectfully submitted,
WILLIAM C. CRILLY, JR.

Dated: August 16, 2011

Daniel P. Burke, (30,735)
DANIEL P. BURKE & ASSOCIATES, PLLC
240 Townsend Square
Oyster Bay, NY 11771
Telephone: (516) 802-0560
Facsimile: (516) 802-0562